REMARKS

Claims 3-26 are pending in this application, with claims 3-10 being independent. Claims 1 and 2 have been canceled, and claims 22-26 have been added. Claims 6-10 and 20 have been amended. Care has been taken to avoid introduction of new matter. Favorable reconsideration of the application in light of the following comments is respectfully solicited.

Allowable Subject Matter

The indication of the allowed claims 3-5 and 11-13 is acknowledged and appreciated. For the reasons that follow, it is respectfully submitted that all pending claims are allowable over the cited references.

Claim Rejections – 35 U.S.C. § 112

Claims 6-10 and 14-21 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Claims 6-10 and 20 have been amended to overcome the above-stated rejection. Accordingly, Applicants respectfully request reconsideration and withdrawal of the § 112, second paragraph, rejection of claims 6-10 and 14-21.

Claim Rejections – 35 U.S.C. § 103

Claim 6 was rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,237,616 ("Abraham"), U.S. Patent 6,101,586 ("Ishimoto"), and U.S. Patent 5,414,864 ("Koizumi). Claims 7, 8, and 10 were rejected under § 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, U.S. Patent Number 5,680,581 ("Banno"), and U.S. Patent Number 5,386,552 ("Garney"). Claim 9 was rejected under § 103(a) as being unpatentable over

Abraham, Ishimoto, Koizumi, and Banno. Applicants respectfully traverse these rejections for at least the following reasons. The following remarks first address the rejection of claim 6, then address the rejection of claim 9, and finally address the rejection of claims 7, 8, and 10.

Applicants previously argued that the cited prior art references fail to describe or suggest a secure bit generating unit for appending a secure bit to the received data. In particular, Applicants argued that because a secure bit is appended to the received data when arithmetic operation or data transfer is performed through a general purpose register or a built-in memory, unlike in the prior art, data does not need to be protected by a privileged mode or a privileged status, and access is not limited according to the types of memory spaces. In response, the Office Action seems to acknowledge that the cited references fail to describe or suggest such a feature; however, the Office Action rejects claims 6-10 for lacking the recitation of data management by appending a secure bit to the accessed data. *See e.g.*, Office Action at page 12, lines 1-7.

To overcome this rejection, Applicants have amended claims 6-10 to explicitly recite that the secure bit is appended to the claimed data. In particular, as amended, claim 6 recites an information processing apparatus for accessing memory spaces including a user memory space and a secure memory space. The information processing apparatus includes a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, adding a secure bit to the received data based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit.

The general purpose register has a function of receiving and holding the data with the secure bit added thereto. The information processing apparatus further includes a built-in RAM space for receiving and holding the data with the secure bit from the general purpose register and delivering the data with the secure bit to the general purpose register and a data output control unit having a function of controlling a data transfer to an external space by using the secure bit.

Applicants respectfully request reconsideration and withdrawal of the rejection of claim 6 because Abraham, Ishimoto, and Koizumi, either alone or in combination, fail to describe or suggest an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, *adding a secure bit to the received data* based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit, the general purpose register having a function of receiving and holding *the data with the secure bit added thereto*, as recited in claim 6.

In Abraham, the information processing apparatus permits a computer to be operated in either a privileged state or an unprivileged state. Abraham at Abstract. In the privileged state, the microprocessor works with a privileged memory (105) and no data or addresses of the memory are accessible outside the secure module represented by a boundary (101) in FIG. 1. Abraham at col. 2, lines 61-65. In the unprivileged state, the microprocessor works only with a memory (109) and data, addresses, and programs in the privileged memory (105) is made unavailable. Abraham at col. 2, lines 65-67.

As such, Abraham describes an information processing apparatus in which addresses of data in memory spaces determine the privileged or unprivileged states. However, Abraham does not describe or otherwise suggest an information processing apparatus including a secure bit generating unit for adding a secure bit to the received data based on the address associated with the received data, and a general purpose register for receiving and holding the data with the secure bit added thereto.

Accordingly, Abraham fails to describe or suggest an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, *adding a secure bit to the received data* based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit, the general purpose register having a function of receiving and holding *the data with the secure bit added thereto*, as recited in claim 6.

As noted above, the distinction is one of the important features of the present application (e.g., data management by appending a secure bit to the accessed data). In particular, because a secure bit is appended to the data, when arithmetic operation or data transfer is performed through a general purpose register or a built-in memory, data does not need to be protected by a privileged mode or a privileged status, and access is not limited according to the types of memory spaces. This can provide several advantages. For example, in a secure memory space, easier data access and arithmetic operation using a program in a user memory space can be achieved. This is quiet an improvement over Abraham and other cited references.

Ishimoto and Koizumi also fail to describe or suggest the above-recited feature of claim 6. Ishimoto relates to a memory access control circuit for inhibiting fraudulent access by detecting an access to a region to be protected on a memory. Ishimoto at col. 12, lines 36-39. The memory access control circuit includes address of data region in the memory that must be protected. Ishimoto at col. 12, lines 43-44. And, if the instructions seek to access this data region, the memory access control checks to determine whether the location of the instruction is within a region in the memory that allows access to the protected region. Ishimoto at col. 12, lines 45-67.

As such, Ishimoto describes a memory access control that provides protection depending on areas where the data is allocated. That is, access to the secured memory is only possible by instructions stored in a particular area in the memory. In contrast and as described below in more detail, the protection mechanism of claim 6, does not limit access based on areas. Rather, in claim 6, the secure bit added to and delivered with the data limits the output of the respective data to an external space.

Accordingly, Ishimoto also fails to describe or suggest an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, *adding a secure bit to the received data* based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit, the general purpose register having a function of receiving and holding *the data with the secure bit added thereto*, as recited in claim 6.

Koizumi also fails to describe or suggest the above-recited features of claim 6. The purpose of Koizumi's invention is to save/store registers using flags that indicate whether or not the register is being used. Koizumi at col. 2, lines 31-42. These protective flags are not added to data but to the register upon instructions to start/stop use of registers. To this end, Koizumi is not seen to have an association with security. Furthermore, the alleged general purpose register in Koizumi does not appear to have any secure bit appended thereto.

Accordingly, Koizumi also fails to describe or suggest an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, *adding a secure bit to the received data* based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit, the general purpose register having a function of receiving and holding *the data with the secure bit added thereto*, as recited in claim 6.

For the foregoing reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 6.

Claim 9 was rejected under § 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, and Banno. Applicants respectfully traverse this rejection.

As amended, claim 9 recites an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, adding a secure bit to the received data based on determining which of the user

memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into the DMA.

Banno fails to remedy the shortcomings of Abraham, Ishimoto, and Koizumi to describe or suggest the above-recited features of claim 9. Banno describes protecting data read from a CPU. Similar to Ishimoto, Banno data protection/non protection is also executed depending on areas where data is located. *See e.g.,* Banno at col. 3, lines 44-61. As such, Banno also fails to describe or suggest limiting the output of the respective data to an external space by delivering the data with one or more secure bits. For at least this reason, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 9.

Claims 7, 8, and 10 were rejected under § 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, Banno, and Garney. Applicants respectfully traverse this rejection for at least the following reasons.

As amended, claim 7 recites an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, adding a secure bit to the received data based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit. The general purpose register has a function of receiving and holding the data with the secure bit added thereto. The secure bit generating unit is also configured to deliver an instruction with a secure bit into an instruction decoder including a secure bit unit. The instruction decoder has a function of determining which of the user memory space and the secure memory space is associated with the instruction under execution.

Applicants respectfully submit that Garney fails to remedy shortcomings of Abraham, Ishimoto, Koizumi, and Banno to describe or suggest the above-recited features of claim 7. Garney is intended for efficient preservation of CPU's processing state in a computer system with volatile memories and registers. Garney is not seen to describe or suggest anything about securing data, much less describing adding a secure bit to the data based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, as recited in claim 7. For at least this reason, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 7.

Claim 8 recites an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space and the secure memory space is indicated by address information associated with the received data, adding a secure bit to the received data based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit. The general purpose register has a function of receiving and holding the data with the secure bit added thereto. The secure bit generating unit is also configured to deliver an instruction with a secure bit into an instruction decoder including a secure bit unit. The instruction decoder has a function of determining which of the user memory space and the secure memory space is associated with the instruction under execution.

Therefore, for at least the reasons presented above with respect to claim 7, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 8.

Claim 10 recites an information processing apparatus that includes, among other features, a secure bit generating unit for receiving data and determining which of the user memory space

and the secure memory space is indicated by address information associated with the received data, adding a secure bit to the received data based on determining which of the user memory space and the secure memory space is indicated by the address information associated with the received data, and delivering the received data with the secure bit into a general purpose register including a secure bit unit. The general purpose register has a function of receiving and holding the data with the secure bit added thereto. The secure bit generating unit is also configured to deliver an instruction with a secure bit into an instruction decoder including a secure bit unit. The instruction decoder has a function of determining which of the user memory space and the secure memory space is associated with the instruction under execution. Therefore, for at least the reasons presented above with respect to claim 7, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 10.

Dependent Claims

Under Federal Circuit guidelines, a dependent claim is nonobvious if the independent claim upon which it depends is allowable because all the limitations of the independent claim are contained in the dependent claims, *Hartness International Inc. v. Simplimatic Engineering Co.*, 819 F.2d at 1100, 1108 (Fed. Cir. 1987). Because claims 6-10 are allowable for the reasons set forth above, it is respectfully submitted that all claims dependent thereon are also allowable. In addition, it is respectfully submitted that the dependent claims are allowable based on their own merits by adding novel and non-obvious features to the combination.

Based on the foregoing, it is respectfully submitted that all pending claims are patentable over the cited prior art. Accordingly, it is respectfully requested that the rejection under 35 U.S.C. § 103 be withdrawn.

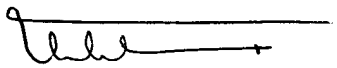
Conclusion

Having fully responded to all matters raised in the Office Action, Applicants submit that all claims are in condition for allowance, an indication for which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicants' attorney at the telephone number shown below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. .1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Babak Akhlaghi
Limited Recognition No. L0250

Please recognize our Customer No. 53080 as our correspondence address.

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 BA:MaM
Facsimile: 202.756.8087
DATE: July 15, 2008